Відповідно до ст. 22 ГК України держава реалізує право державної власності у державному секторі економіки через систему організаційно-господарських повноважень відповідних органів управління щодо суб'єктів господарювання, що належать до цього сектора і здійснюють свою діяльність на основі права господарського відання або права оперативного управління [1].

Оскільки Державна авіаційна служба України є центральним органом державної виконавчої влади, вона також реалізовує організаційно-господарські повноваження щодо суб'єктів господарювання, які належать до сфери її управління.

Відповідно до п. 4 Положення про Державну авіаційну службу України Державіаслужба відповідно до покладених на неї завдань забезпечує створення рівних умов для розвитку господарської діяльності підприємств цивільної авіації усіх форм власності [2].

Таким чином, основні функції та завдання Державної авіаційної служби України як органу господарського керівництва визначені у Конституції України, Господарському кодексі Україні, Законі України «Про ліцензування видів господарської діяльності», Положенні про Державну авіаційну службу України та інших нормативно-правових актах.

Література

1. Господарський кодекс України від 16.01.2003 р., № 436-IV // Відомості Верховної Ради України. – 2003. – № 18. – Ст. 144.

2. Про затвердження Положення про Державну авіаційну службу України: Постанова Кабінету Міністрів України від 08.10.2014 р. № 520 // Офіційний вісник України. – 2014. – № 82. – Ст. 63.

УДК 342.9

Діордіца І. В., к.ю.н., доцент,
Академія праці, соціальних відносин і туризму, м. Київ, Україна

КОНЦЕПТ-ПРОДУКТ КІБЕРШПИГУНСТВА У ГЛОБАЛЬНОМУ СВІТІ

Останніми роками все більшу занепокоєність уряду України та провідних країн світу викликає збільшення та поширення фактів кібершпигунства. Так, у минулорічному докладі керівника Управління національної контррозвідки США звинувачуються, зокрема Росія у зборі інформації, а Китай безпосередньо у промисловому та економічному шпигунстві, що здійснюються за допомогою комп'ютерних технологій [1].

У світлі останніх подій можна зазначити і про такі прояви кібершпигунства.

В 2015 році була виявлена атака на Офіс управління кадрами, що

розпочалась в березні 2014 року. Було викрадено особисту інформацію близько 21,5 млн осіб, переважно федеральних працівників, зокрема інформацію про перевірки на доступ до таємної інформації. Американські посадовці назвали її найбільшою атакою в історії Сполучених Штатів. У цьому ж році була виявлена кібератака на інформаційну систему Бундестагу; серед інших, вірусом був вражений комп'ютер федерального канцлера Німеччини Анґели Меркель. Відповідальність за атаку дослідники покладають на російське угрупування кіберзлочинців англ. Sofacy Group (також відоме як англ. Pawn storm), яких вважають пов'язаними з російськими спецслужбами. Це ж угрупування намагалось зламати інформаційні системи Ради безпеки Нідерландів аби отримати доступ до інформації про перебіг розслідування збиття літака рейсу MH17 [2].

31 липня кандидат у Президенти США Гіларі Клінтон заявила про злам комп'ютерів комітетів партії хакерами російських спецслужб.

2 вересня 2016 року було заявлено про злам комп'ютерної системи у Всесвітньому антидопінговому агентстві.

Листопад 2016 року – серйозна кібератака на ОБСЄ. Хакери могли отримати доступ до електронної пошти співробітників організації та до її баз даних. Видавництво Le Monde із посиланням на західні спецслужби також повідомило, що дану атаку, організувала хакерська група APT28 (Fancy Bears), відома своїми зв'язками із російськими спецслужбами [3].

У червні 2016 стало відомо про виявлення несанкціонованого втручання до інформаційної системи Національного комітету Демократичної партії США. Несанкціоноване втручання було виявлене іще наприкінці квітня, тоді ж до розслідування була залучена фірма CrowdStrike. В результаті проведеного розслідування було встановлено, що зламати інформаційну систему вдалось двом угрупуванням російських хакерів – Cozy Bear (CozyDuke або APT29) та Fancy Bear (Sofacy Group або APT28). Група Cozy Bear проникла до інформаційної системи іще влітку 2015 року, а Fancy Bear – в квітні 2016 року. Обидва угрупування спромоглись викрасти скриньки електронної пошти а також зібраний компромат на конкурента демократів на виборах – Дональда Трампа.

У липні 2016 року була оприлюднена доповідь, згідно з якою китайські хакери отримали та зберігали несанкціонований доступ до інформаційної системи Федеральної корпорації гарантування вкладів США (англ. FDIC) з 2010 до 2013 роки. Високопосадовці у FDIC намагались приховати інформацію про злам системи від ревізорів та контролюючих органів. Китайські хакери, пов'язані з китайським урядом, отримали доступ до 12 персональних комп'ютерів та 10 серверів, включно з комп'ютерами найвищого керівництва FDIC. На FDIC покладена роль банківського регулятора для банків, які не регулюються Федеральною резервною системою США. В ній зберігається надзвичайно чутлива

інформація про близько 4500 банків та інших кредитних установ. Також FDIC гарантує вклади осіб у всіх банках країни.

13 серпня 2016 року досі невідоме угрупування, яке назвало себе англ. The Shadow Brokers розмістило в репозиторії GitHub, сайті PasteBin а також в соціальних мережах Twitter й Tumblr повідомлення про успішний злам інформаційних систем й викрадення даних іншого хакерського угрупування – Equation Group. Частина викрадених файлів була викладена у відкритий доступ, а частину новоявлена група розмістила на аукціон, з початковою ставкою 1 млн біткоінів (близько $568 млн). Серед викладених у відкритий доступ файлів знаходились скрипти для установки й налаштування серверів управління шкідливим ПЗ, а також інструменти для атаки на окремі мережеві маршрутизатори й екрани. Назви деяких з цих інструментів збігаються з інструментами, згаданими в документах, викрадених перебіжчиком до Росії Едвардом Сноуденом [2].

Констатуємо, що в арсеналі кібершпигунства використовується значна кількість методів ведення своєї діяльності.

Наприклад, державні служби Японії та США спеціально співпрацюють із розробниками додатку на смартфони Pokemon Go, щоб у такий спосіб дізнатись більше про військові й таємні об’єкти різних країн, адже наявність покемонів змусить користувачів робити фотографії в таких місцях. Представництво компанії Niantic заперечило обвинувачення, що гра може бути інструментом розвідки та закликала всіх користувачів дотримуватись місцевих законів, поважати локації, які вони відвідують, і людей, яких зустрічають.

Хамбі Бакхіт (Hamdi Bakheet), член Єгипетського комітету оборони й національної безпеки, заявив у парламенті: «Pokemon Go – це найновіший інструмент, який використовують шпигунські мережі у війнах, підступний додаток, який намагається просочитись у наші спільноти …».

Індонезійські чиновники називають гру загрозою національній безпеці, оскільки вона може дозволити ворогам проникнути в таємні об’єкти й дістати доступ до секретних матеріалів.

Збройні сили Ізраїлю заборонили солдатам користуватись додатком Pokemon Go на території військових баз.

Оскільки влада Південної Кореї ще раніше заборонила Google Maps, уважаючи їх загрозою національній безпеці, то Pokemon Go, яка використовує дані звідти, не змогла б функціонувати тут. Однак гра несподівано запрацювала в невеликому містечку Сокчхо, що пояснюють помилкою картографічної частини програми та помилковим спрямуванням її в регіон, куди входить Північна Корея [4].

Ціла низка вітчизняних підприємств, порушення роботи яких може становити загрозу життю та здоров’ю громадян, може стати потенційною ціллю для здійснення терористичних актів, в тому числі – із застосування сучасних інформаційних технологій. Не меншою загрозою є вчинення

протиправних дій на шкоду третім країнам, що здійснюються із використанням вітчизняної інформаційної інфраструктури, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Інформація з обмеженим доступом, що циркулює в національних інформаційних ресурсах є стійким об'єктом зацікавленості з боку інших держав, організацій та осіб. Крім того, все більшого поширення набуває політично вмотивована діяльність в кіберпросторі груп активістів (хактивістів), які здійснюють атаки на урядові та приватні сайти, що призводить до порушень роботи інформаційних ресурсів, а також репутаційних та матеріальних збитків.

Література

1. Контрразведка США обвиняет Китай и Россию [Електронний ресурс]. – Режим доступу: http://www.russian.rfi.fr/v-mire/20111104-kontrrazvedka-ssha-obvinyaet-kitaya-i-rossiyu.

2. Вікіпедія [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%.

3. Режим доступу: https://www.google.com/url?hl=ru&q=http://m.gordonua.com/news/worldnews/v-obse-podtverdili-sereznuyu-kiberataku-na-organizaciyu166462.html&source=gmail&ust=1483818224283000&usg=AFQjCNEUyKXN61bK5W50TOJ5_L40UiKDBQ.

4. Наступ покемонів: чому влади деяких країн проти Pokemon Go [Електронний ресурс]. – Режим доступу: http://osvita.mediasapiens.ua/ media_law/government/nastup_pokemoniv_chomu_vladi_deyakikh_krain_proti_pokemon_go/.

УДК 347.85

Доценко В. О., д.і.н., професор,
Шевченко А. Є., д.ю.н., професор,
Університет державної фіскальної
служби України, м. Ірпінь, Україна

ПРАВОВІ ПРОБЛЕМИ ЗДІЙСНЕННЯ КОСМІЧНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

В останні роки в Україні намітились тенденції до розвитку міжнародного і національного космічного права. Сьогодні Україна оцінює питання розвитку космічного права як надзвичайно актуальні. Від них у багатьох випадках залежить продуктивність здійснення космічної діяльності, успішність участі держави у розвитку світового космічного ринку.

Економічний розвиток України напряму залежить від створення власної космічної інфраструктури, модернізації радянського спадку та